

REMARKS

Claims 1-8 are pending in the present application. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Objection to the Specification

By this Response, the specification is amended to correct minor informalities. The specification is amended to recite "A Certification Authority (CA) guarantees the identity of the owner of the pair of keys (the development laboratory in the example at issue) by means of a corresponding digital certificate." Applicants are only amending the specification to satisfy the Examiner's Objection to the Specification and no new matter has been added.

II. 35 U.S.C. § 112, Second Paragraph, Claims 1-8

The Office Action rejects claims 1-8 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which Applicants regard as the invention. This rejection is respectfully traversed.

With regard to claims 1-8, the Office Action states:

Claims 1-8, are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Both independent claims contain the term "entity" however it is not clear if the term 'entity' applies to the client or product. Appropriate correction is required. The dependent claims 2-7 are rejected based on there dependency to the independent claim 1.

(Office Action dated May 9, 2008, page 2)

The question raised in the Office Action with regard to claims 1 and 8 is to illustrate how the claim is allegedly indefinite. Determining whether a claim is indefinite requires an analysis of whether one skilled in the art would understand the bounds of the claim when read in light of the specification. *Credle v. Bond*, 25 F.3d 1566, 1576, 30 U.S.P.Q.2d 1911, 1919-1920 (Fed. Cir. 1994). As long as the claim language is clear on

its face and informs those of ordinary skill in the art of the metes and bounds of the claim scope, there is no indefiniteness.

As stated in MPEP § 2173.02:

The examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is **whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available.** When the examiner is satisfied that patentable subject matter is disclosed, and it is apparent to the examiner that the claims are directed to such patentable subject matter, he or she should allow claims which define the patentable subject matter with a **reasonable degree of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire.** Examiners are encouraged to suggest claim language to applicants to improve the clarity or precision of the language used, but should not reject claims or insist on their own preferences if other modes of expression selected by applicants satisfy the statutory requirement.

The essential inquiry pertaining to this requirement is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity. Definiteness of claim language must be analyzed, not in a vacuum, but in light of:

- (A) The content of the particular application disclosure;
- (B) The teachings of the prior art; and
- (C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made.

In reviewing a claim for compliance with 35 U.S.C. 112, second paragraph, the examiner must consider the claim as a whole to determine **whether the claim apprises one of ordinary skill in the art of its scope** and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph, by providing clear warning to others as to what constitutes infringement of the patent. See, e.g., *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1379, 55 USPQ2d 1279, 1283 (Fed. Cir. 2000). See also *In re Larsen*, No. 01-1092 (Fed. Cir. May 9, 2001) (unpublished) (The preamble of the *Larsen* claim recited only a hanger and a loop but the body of the claim positively recited a linear member. The court observed that the totality of all the limitations of the claim and their interaction with each other must be considered to ascertain the inventor's contribution to the art. Upon review of the claim in its entirety, the court concluded that the claim at issue apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35

U.S.C. 112 paragraph 2.). >See also *Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1366, 71 USPQ2d 1081, 1089 (Fed. Cir. 2004) (“**The requirement to ‘distinctly’ claim means that the claim must have a meaning discernible to one of ordinary skill in the art when construed according to correct principles....Only when a claim remains insolubly ambiguous without a discernible meaning after all reasonable attempts at construction must a court declare it indefinite.**”). (emphasis added)

Applicants respectfully submit that the claim satisfies the “threshold requirements of clarity and precision,” “set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity,” and “apprises one of ordinary skill in the art of its scope.” Claim 1, which is representative of the other rejected dependent claim 8 with regard to similarly recited subject matter, reads as follows:

1. A method of authenticating a digitally encoded **product being originated by an entity** having at least one authorized subject, the method including the steps of:
 - a client system transmitting a request of authentication of the product to a server system,
 - the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:
 - certifying that the product originates from the **entity** using sensitive information of the entity stored on the server system, and
 - returning a representation of the certification to the client system. (emphasis added)

There is nothing indefinite about certifying that the product originates from the entity. Looking at the preamble of the claim, it is clear that the product originated from the entity and in order to certify that the product originates from the entity, the client system transmits a request of authentication of the product to a server system, the server system verifies whether the request is received from an authorized subject, and responsive to a positive verification: the server system certifies that the product originates from the entity using sensitive information of the entity stored on the server system, and returns a representation of the certification to the client system. The language is not unclear and one of ordinary skill in the art is perfectly capable of discerning that the product originated from the entity and the presently claimed invention is directed to certifying that the product originates from the entity.

The claim limitation is sufficient to enable those skilled in the art to draw a line between embodiments falling within the scope of the claim and those which do not. *In re Marosi*, 710 F.2d 799, 802-03, 218 U.S.P.Q. 289, 292 (Fed. Cir. 1983). The claims may be broad, but they are clear and are not indefinite as to what Applicants regard as their invention. However, in an effort to aid the Examiner, the current specification clearly sets forth, as part of an exemplary illustrative embodiment, why it is necessary to certify that the product originates from the entity, for example, on page 6, line 23, to page 7, line 4, and elsewhere. The exemplary section of page 6, line 23, to page 7, line 4, of the current specification reads as follows:

The digital signature of a message is created generating a hash value of the message. The hash value consists of a pre-set number of bits, lower than the one required to encode the message directly; nevertheless, the hash value is substantially unique for the message (that is, any change in the message generates a different hash value). The hash value is obtained using a one-way function, so that it is computationally unfeasible to obtain the message from the hash value. The digital signature is then created by encrypting the hash value with the private key of a sender. A receiver of the (signed) message can validate the same simply generating the hash value of the message and comparing this hash value with the one extracted from the digital signature using the public key of the sender. In this way, the receiver verifies that the original message has not been corrupted (integrity) and that it has been actually sent by the entity identified in the digital certificate (authenticity).

As is illustrated in this example, by the receiver of the (signed) message generating a hash value of the message and comparing the hash value with the one extracted from the digital signature using the public key of the sender, the receiver verifies that the original message has not been corrupted and that it has been actually sent by the entity identified in the digital certificate. This is only an example of why it is necessary to certify that the product originates from the entity, and should not be construed, as limiting the present claims.

Therefore, in view of the above, Applicants respectfully submit that claims 1 and 8 are not indefinite and are in condition for allowance. At least by virtue of their dependency on claim 1, the features of dependent claims 2-7 are not indefinite and are in condition for allowance. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-8 under 35 U.S.C. § 112, second paragraph.

III. 35 U.S.C. § 102, Claims 1-3

The Office Action rejects claims 1-3 under 35 U.S.C. § 102(e) as being anticipated by Bhagavatula et al. (U.S. Patent No. 7,140,036 B2). This rejection is respectfully traversed.

Claim 1 reads as follows:

1. A method of authenticating a digitally encoded **product being originated by an entity** having at least one authorized subject, the method including the steps of:
 a client system transmitting a request of authentication of the product to a server system,
 the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:
 certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and
 returning a representation of the certification to the client system. (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that Bhagavatula does not identically show every element of claim 1 arranged as they are in the claim. Specifically, Bhagavatula does not teach the elements emphasized above in claim 1.

Bhagavatula is directed to centralized identity authentication for use in connection with a communications network. Bhagavatula registers users of the communications network such that each registered user's identity is uniquely defined and determinable. Bhagavatula also registers a plurality of vendors having a presence on the communications network. The registered vendors selectively transact with registered

users, wherein the transactions include: (i) the registered vendor selling goods and/or services to the registered user; (ii) the registered vendor granting the registered user access to personal records maintained by the registered vendor; and/or (iii) the registered vendor communicating to the registered user personal information maintained by the registered vendor. The method also includes each user's identity being authenticated over the communications network prior to completion of transactions between registered vendors and registered users.

Thus, Bhagavatula merely authenticates users and vendors that access the communications network. The Office Action alleges that Bhagavatula teaches a client system transmitting a request of authentication of the product to a server system at column 8, lines 20-25, which is reproduced as follows:

On the other hand, if the user 40 passes the authentication procedure 302, the agent 10 administers a request processing procedure 308. The request processing procedure 308 retrieves the information or data requested by the user 40 from the respective vendors 30a-n, and forwards the same back to the user 40, e.g., via a requested information page 310.

(Bhagavatula, column 8, lines 19-25)

In this section, Bhagavatula describes that, in response to a user requesting access to personal and/or confidential information from one or more registered vendors and the user being authenticated by an agent, the agent retrieves the information or data requested by the user from the respective vendors and forwards the data back to the user. Thus, the request sent by the user to the agent is for access to data from a vendor. Bhagavatula merely authenticates that the user “to ensure that the user 40 is registered and is in fact who he claims to be.” (see Bhagavatula, column 7, lines 64-65) Nowhere in this section, or in any other section of Bhagavatula, is there a teaching of a client system transmitting a **request of authentication of the product** to a server system. That is, the request sent to Bhagavatula’s agent is for access to vendor data. Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be.

Additionally, Bhagavatula fails to teach certifying that the product originates from the entity using sensitive information of the entity stored on the server system. The Office Action alleges that Bhagavatula teaches this feature at column 7, line 57 to column 8, line 25, which is reproduced as follows:

By way of example, FIG. 4 shows user 40 accessing personal and/or confidential information from one or more registered vendors 30a-n. An authenticated data access process 300 begins with a registered user 40 contacting the agent 10, preferably, over the Internet 20. The agent 10 conducts an authentication procedure 302 to positively identify the user 40, i.e., to ensure that the user 40 is registered and is in fact who he claims to be. The authentication procedure 302 preferably includes the agent 10 presenting an authentication page to the user 40. The authentication page is set up to collect authentication data from the user 40. Depending on the authentication vehicle set up for the user 40, the authentication data may include a user name or ID, a secret password, a dynamically changing password, a PIN, answers to security questions, biometric data, etc. The authentication data collected by the agent 10 is compared for consistency to the user account information maintained in the agent's database 14, and where there is a match, the user 40 is deemed authentic and positively identified as the holder of the matching account.

At decision step 304, it is determined if the user 40 has passed the authentication procedure 302. If the user 40 has not passed the authentication procedure 302, an access denied page 306 is returned to the user 40 informing him of his failure to be authenticated. Optionally, the access denied page 306 permits the user 40 to change and/or correct previously mis-entered authentication data and try again. The number of tries is, however, preferably limited.

On the other hand, if the user 40 passes the authentication procedure 302, the agent 10 administers a request processing procedure 308. The request processing procedure 308 retrieves the information or data requested by the user 40 from the respective vendors 30a-n, and forwards the same back to the user 40, e.g., via a requested information page 310.

(Bhagavatula, column 7, line 57, to column 8, line 25)

As discussed above, in this section Bhagavatula describes that, in response to a user requesting access to personal and/or confidential information from one or more registered vendors and the user being authenticated by an agent, the agent retrieves the information or data requested by the user from the respective vendors and forwards the data back to the user. Again, the request sent by the user to the agent is for access to data from a vendor. Nowhere in this section, or in any other

section of Bhagavatula, is there a teaching of certifying that the product originates from the entity using sensitive information of the entity stored on the server system. That is, the request sent to Bhagavatula's agent is for access to vendor data. Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be.

Further, Bhagavatula fails to teach returning a representation of the certification to the client system. The Office Action alleges that Bhagavatula teaches this feature at column 7, line 57 to column 8, line 25, which is reproduced above. As described above, Bhagavatula retrieves **the information or data requested by the user** from the respective vendors and forwards the data back to the user, in response to a user requesting access to personal and/or confidential information from one or more registered vendors and the user being authenticated by an agent. Nowhere in this section, or in any other section of Bhagavatula, is there a teaching of returning a representation of the certification that the product originates from the entity to the client system. Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be.

Therefore, Bhagavatula does not teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(e). At least by virtue of their dependency on independent claim 1, the specific features of dependent claims 2 and 3 are not taught by Bhagavatula. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-3 under 35 U.S.C. § 102(e).

Furthermore, Bhagavatula does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Absent the Office Action pointing out some teaching or incentive to implement Bhagavatula such that a client system transmits a request of authentication of the product to a server system, the server system certifies that the product originates **from an entity** using sensitive information of the entity stored on the server system, and the server system returns a representation of the certification to the client system, as recited in independent claim 1, one of ordinary skill in the art would not be led to modify Bhagavatula to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify Bhagavatula in this manner, the presently claimed invention can be

reached only through an improper use of hindsight using the Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

IV. 35 U.S.C. § 103, Alleged Obviousness, Claims 4-8

The Office Action rejects claims 4-8 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Bhagavatula et al. (U.S. Patent No. 7,140,036 B2) in view of Graves et al. (U.S. Publication No. 2004/0177047 A1). This rejection is respectfully traversed.

Claims 4-7 are dependent on independent claim 1 and, thus, these claims distinguish over Bhagavatula for at least the reasons noted above with regard to claim 1. Moreover, Graves does not provide for the deficiencies of Bhagavatula and, thus, any alleged combination of Bhagavatula and Graves would not be sufficient to reject independent claim 1 or claims 4-7 by virtue of their dependency. That is, Bhagavatula and Graves, taken alone or in combination, do not teach or suggest transmitting from a client system a request of authentication of the product to a server system, certifying by a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and returning by a server system a representation of the certification to the client system.

Furthermore, Bhagavatula and Graves, taken alone or in combination, fail to teach or suggest the features of claims 4-7. For example, with regard to claim 4, Bhagavatula and Graves, taken alone or in combination, do not teach or suggest where the step of certifying that the product originates **from an entity** using sensitive information of the entity stored on the server system includes automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key. The Office Action acknowledges that Bhagavatula does not teach these features, but alleges that Graves teaches where the step of certifying that the product originates **from an entity** using sensitive information of the entity stored on the server system includes automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key.

Graves is directed to an online commerce transaction system that authenticates to a seller that a buyer is authorized to use a payment instrument as part of an online

commerce transaction with the seller. The authentication service performs the following receives a request to verify that the buyer is authorized to use the payment instrument. The authentication service determines whether the buyer has access to certain secret information without revealing the secret information to the seller. Access to the secret information verifies authority to use the payment instrument. Responsive to the determination of whether the buyer has access to the secret information, the authentication service transmits to the seller a response including whether the buyer is authorized to use the payment instrument.

Thus, Graves merely describes authenticating whether a user is authorized to use the payment instrument. The Office Action alleges that Graves teaches where the step of certifying that the product originates **from an entity** using sensitive information of the entity stored on the server system includes automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key in paragraphs [0050], [0052], and [0053], which are reproduced as follows:

[0050] The PTA and private keys may be hosted in a number of locations. In this example, a separate server (not shown) hosts the software implementing the PTA and stores the corresponding private keys. One advantage of this approach is that since the PTA and private keys are implemented as a zero-client, hosted service, no changes need be made to the buyer's browser. Another advantage is that since the buyer's browser does not require any special software, the buyer 110 potentially can access the PTA and his private keys from any standard browser. For an example of how this may be implemented, see co-pending U.S. patent application Ser. No. 09/574,687, "Server-Assisted Regeneration of a Strong Secret from a Weak Secret," by Warwick Ford, filed May 17, 2000, which subject matter is incorporated herein by reference. If the server hosting the PTA is the same as the one hosting the authentication service 130, the two functions may be integrated to some degree. In an alternate embodiment, the PTA and/or corresponding private keys are implemented on the buyer's client. For example, the PTA may be implemented as a plug-in (e.g., ActiveX control) to the buyer's browser and the private keys stored locally on the buyer's client or in dedicated hardware (e.g., a hardware token).

[0052] As a result of clicking the authenticated payment button 420, a request for authentication is sent 330 from the buyer's browser to the authentication service 130. The request includes a description of the payment transaction and also identifies the seller 120. The authentication service 130 determines whether the buyer 110 has access to the secret

information (in this case, the private key for the selected account) in steps 340-346. In particular, the authentication service 130 sends 340 a challenge request to the buyer 110. The challenge request asks the buyer 110 to digitally sign some data using the private key for the selected account. The buyer 110 sends 342 his challenge response back to the authentication service 130. The authentication service 130 retrieves the earlier stored public key and uses it to determine 346 whether the buyer 110 has access to the corresponding private key. The authentication process typically is carried out between computers without the human buyer 110's active participation.

[0053] In this embodiment, the PTA is also invoked in order to allow the buyer 110 to select which of his accounts he wishes to use and later to select the specific payment instrument from within the account. More specifically, clicking button 420 causes the buyer's web browser to interact with the PTA via the dialog boxes in FIGS. 5A and 5B. In FIG. 5A, the buyer 110 specifies which account he wishes to use by filling in the User Name field 510 and then authenticates himself to the PTA by filling in the correct password 520. The PTA displays the dialog box of FIG. 5B, which includes a visual representation 530 of the account selected. The buyer 110 confirms that he wishes to use this account by clicking on the Login button 540. The private key for the account is now available for authentication and digital signature.

(Graves, paragraphs [0050], [0052], and [0053])

In these paragraphs, Graves describes that, responsive to clicking an authenticated payment button, a request for authentication is sent from the buyer's browser to the authentication service. The request includes a description of the payment transaction and also identifies the seller. The authentication service determines whether the buyer has access to the secret information. The authentication service sends a challenge request to the buyer. The challenge request asks the buyer to digitally sign some data using the private key for the selected account. The buyer sends his challenge response back to the authentication service. The authentication service retrieves the earlier stored public key and uses it to determine whether the buyer has access to the corresponding private key.

Applicants respectfully submit that Graves authentication service does not automatically retrieve a private key of the entity from which the product originates that is stored on the server system in order to certify that the product originates **from an entity** using sensitive information of the entity stored on the server system. That is, Graves' authentication service receives a request from a buyer **that authenticates whether a user**

is authorized to use the payment instrument. The certificate does not certify that the product originates **from an entity** using sensitive information of the entity stored on the server system.

Additionally, with regard to claim 7, Bhagavatula and Graves, taken alone or in combination, do not teach or suggest the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, and the server system executing the remote command if included in the list. The Office Action alleges that Graves teaches this feature in paragraphs [0050], [0052], and [0053], which are reproduced above. As described above, Graves merely authenticates whether a user is authorized to use the payment instrument. Applicants respectfully submit that Graves' authentication service does not verify whether the remote command is included in a predefined list stored on the server system. At most, Graves merely sends a challenge request to the buyer, asks the buyer to digitally sign some data using the private key for the selected account, sends this challenge response back to the authentication service, and retrieves the earlier stored public key and uses it to determine whether the buyer has access to the corresponding private key. Nowhere in the Graves reference is there a teaching or suggestion that the certificate from the user is compared to a list of certificates much less a list that includes at least one remote command for satisfying the request of authentication.

With respect to claim 8, similar distinctions of the claims over the Bhagavatula as discussed above with respect to claim 1, apply to independent claim 8. Claim 8 recites “**a client system transmitting a request of authentication of the product to a server system, the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification: generating a digital signature of the product using a private key of the entity stored on the server system, and returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity.**” (emphasis added). Graves does not provide for the deficiencies of Bhagavatula and, thus, any alleged combination of Bhagavatula and Graves would not be sufficient to reject independent claim 8. That is, Bhagavatula and Graves, taken alone or in combination, do not teach or suggest transmitting from a client

system a request of authentication of the product to a server system, certifying by a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and returning by a server system a representation of the certification to the client system.

The Office Action alleges that Graves teaches generating a digital signature of the product using a private key of the entity stored on the server system in paragraphs [0050], [0052], and [0053], which are reproduced above. Again, in these sections, Graves merely authenticates whether a user is authorized to use the payment instrument. Applicants respectfully submit that one of ordinary skill in the art would not confuse Grave's generation of authentication challenge for a buyer to that authenticates whether a user is authorized to use the payment instrument with the presently claimed generating a digital signature of the product that certifies that the product originates **from an entity** using sensitive information of the entity stored on the server system.

Additionally, the Office Action alleges that Graves teaches returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity in paragraph [0056], which is reproduced as follows:

[0056] The buyer 110 and authentication service 130 create 380 a digitally signed record of the transaction using the form and dialog box shown in FIGS. 7A and 7B. In response to the submission of the form 600, the authentication service 130 returns the form of FIG. 7A which contains a summary 710 of the transaction and requests that the buyer 110 authorize the transaction. The buyer 110 does so by clicking on the Authorize Transaction button 720. This invokes the PTA dialog box of FIG. 7B. By clicking the Sign button 730, the buyer causes the PTA to digitally sign the summary, thus creating a digitally signed record of the transaction. The authentication service 130 then notifies 350 the seller 120 that the buyer is authorized to use the payment instrument and preferably also notifies the buyer that the transaction was approved.

(Graves, paragraphs [0056])

In this paragraph, Graves describes creating a digitally signed record of a transaction and the authentication service returning a form which contains a summary of the transaction and requests that the buyer authorize the transaction. Applicants respectfully submit one of ordinary skill in the art would not confuse returning a record

of transaction with returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity.

Furthermore, no suggestion is present in any of the references to modify the references to include such a feature. That is, there is no teaching or suggestion in Bhagavatula and Graves, taken alone or in combination, that a problem exists for which transmitting from a client system a request of authentication of the product to a server system, certifying by a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and returning by a server system a representation of the certification to the client system, is a solution. To the contrary, Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be. Graves merely describes authenticating whether a user is authorized to use the payment instrument. Neither of the references certifies at a server system that **a product originates from an entity** using sensitive information of the entity stored on the server system.

Moreover, neither reference teaches or suggests the desirability of incorporating the subject matter of the other reference. That is, there is no motivation offered in either reference for the alleged combination. The Office Action alleges that the motivation would be “because there is a need for buyer authentication in online purchase.” The present invention provides for a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system. As discussed above, Bhagavatula merely authenticates the user to ensure the user is registered and is in fact who he claims to be and Graves merely describes authenticating whether a user is authorized to use the payment instrument. Neither reference teaches or suggests transmitting a request of authentication of the product to a server system, a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system, and a server system returning a representation of the certification to the client system. Thus, the only teaching or suggestion to even attempt the alleged combination is based on a prior knowledge of Applicants’ claimed invention thereby constituting impermissible hindsight reconstruction using Applicants’ own disclosure as a guide.

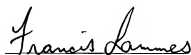
One of ordinary skill in the art, being presented only with Bhagavatula and Graves, and without having a prior knowledge of Applicants' claimed invention, would not have found it obvious to combine and modify Bhagavatula and Graves to arrive at Applicants' claimed invention, as recited in claims 1 or 8. To the contrary, even if one were somehow motivated to combine Bhagavatula and Graves, and it were somehow possible to combine the systems, the result would not be the invention as recited in claims 1 or 8. The resulting system would be verifying that a user has access to download the executable file prior to downloading the file. The resulting system would still fail to transmit a request of authentication of the product to a server system, certify at a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and return from a server system a representation of the certification to the client system.

In view of the above, Applicants respectfully submit that Bhagavatula and Graves, taken alone or in combination, fail to teach or suggest the features of claim 1 and 8. At least by virtue of their dependency on independent claim 1, the specific features of dependent claims 4-7 are not taught or suggest by Bhagavatula and Graves, either alone or in combination. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 4-8 under 35 U.S.C. § 103(a).

V. **Conclusion**

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

A handwritten signature in cursive script, reading "Francis Lammes", written in dark ink.

DATE: June 17, 2008

Francis Lammes
Reg. No. 55,353
WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6491
AGENT FOR APPLICANTS